REMARKS

A. INTRODUCTION

The Office Action has been received and carefully considered. Claims 1-25 are pending in the application. In this response, no amendment has been made to the claims or other parts of the application. Applicant believes that the application is in condition for allowance and notice thereof is respectfully requested.

B. THE REJECTION UNDER 35 U.S.C. § 103

The Office Action rejects claims 1-2, 11-13 and 25 under 35 U.S.C. §103(a) as being unpatentable over Sit *et al.* (US Patent 6,349,336, hereinafter "Sit") in view of Epstein *et al.* (US Patent 6,584,508, hereinafter "Epstein"). The Office Action also rejects claims 3-4 and 14-15 under 35 U.S.C. §103(a) as being unpatentable over Sit, Epstein and further in view of Fan *et al.* (US Patent 6,219,706, hereinafter "Fan"). The Office Action further rejects claims 5-10 and 16-24 under 35 U.S.C. §103(a) as being unpatentable over Sit, Epstein, Fan and further in view of Albert *et al.* (US Patent 6,687,222, hereinafter "Albert").

These rejections are improper for at least the following reasons. (1) The combinations of Sit with the other references fail to teach or suggest all the elements in the claimed invention. (2) There is no suggestion or motivation in the cited references or in the general knowledge to make the combinations.

Applicant's invention, as recited in independent claims 1 and 12, is directed to a secured file transfer protocol (FTP) system and method. Embodiments of the present invention specifically address the difficulties faced by a FTP client behind a firewall. In one embodiment, two FTP proxy systems (e.g., a FTP client proxy system 12 and a FTP server agent 14 in Figure 2) are positioned astride a firewall device. The client-side FTP proxy system (e.g., the FTP

client proxy system 12) has a FTP-like session with the FTP client. The server-side FTP proxy system (e.g., the FTP server agent 14) has a FTP-like session with the FTP server. The two FTP proxy systems communicate with each other securely across the firewall device via a single port thereon. One advantage of such an embodiment is to prevent the firewall from opening and closing random ports as in traditional FTP sessions.

Sit discloses a hypertext transfer protocol (HTTP) tunneling action that allows a remote processor to communicate with a local processor when the remote processor is coupled to the local processor via a reverse proxy device, a computer network, a firewall and a proxy agent device. The primary goal in Sit is to trick the firewall into believing that an incoming request is actually a response to an outgoing request, so that the remote processor may access/control the local processor behind the firewall. See Sit: col. 2, lines 39-60 and col. 3, lines 36-48.

Epstein discloses an advanced data guard having independently wrapped components. One of the independently wrapped components may be a FTP proxy. See Epstein: Figure 4.

Applicant's following arguments regarding the primary references Sit and Epstein will moot the obviousness rejections further based on Fan and Albert.

(1) The Sit-Epstein Combination Fails to Teach or Suggest All the Elements in the Claimed Invention.

As stated in MPEP § 2143.03, to establish *prima facie* obviousness of a claimed invention, all the claim limitations must be taught or suggested by the prior art. In re Royka, 490 F.2d 981, 180 USPQ 580 (CCPA 1974). That is, "[a]ll words in a claim must be considered in judging the patentability of that claim against the prior art." In re Wilson, 424 F.2d 1382, 165 USPQ 494, 496 (CCPA 1970).

Individually or in combination, Sit and Epstein do not teach or suggest "*restricting [FTP] data flow between said first proxy system and said second proxy system to outbound*

communications through a single port on said firewall" or "*restricting all flow of FTP data passing through said security system through a single port on said firewall.*" Claim 12. See also, Claim 1.

A search of the Sit patent description reveals that Sit never uses the terms "port" or "FTP" or "file transfer protocol." Though Epstein mentions "ports" or "TCP/IP ports" several times, none of those are in the context of FTP. Nor does Epstein provide any teaching or suggestion of restricting data flow to a single port in a firewall.

In the Office Action, the Examiner appears to suggest that the following passage in Sit teaches single-port FTP through a firewall:

> "Reverse [sic] proxy agent 306 (hereafter "agent") initiates a connection, in response to a request received from a Web server 308I, through the firewall to a reverse proxy device 312 positioned on the external side 304 of firewall 305. This connection is kept open until the user closes the connection." Sit, col. 7, lines 34-40.

However, this interpretation of Sit ignores the context in which the connection is described.

In its proper context, the quoted passage only shows that the two proxy devices are in "persistent connection" with each other while servicing a HTTP session. It has no relevance whatsoever to FTP sessions through a firewall as addressed in the claimed invention. A "persistent connection" between an HTTP client and an HTTP server is mandated by HTTP/1.1 standard, which specifies that "HTTP implementations SHOULD implement persistent connections." Fielding, et al., Hypertext Transfer Protocol -- HTTP/1.1, Network Working Group RFC-2616, June 1999, page 43. Thus, there is nothing remarkable about a persistent HTTP connection between the two proxy systems, as the single connection is the norm for an HTTP session, whether or not it is through a firewall.

For an FTP session, on the other hand, a single-port connection through a firewall was not the norm at the time of the present invention. In many ways, an FTP session through a firewall is completely different from an HTTP session through a firewall. First, a typical FTP session needs at least two TCP connections, one control connection and one data connection. Postel et al, FILE TRANSFER PROTOCOL (FTP), Network Working Group STD-9 (RFC-959), October 1985, pages 3 and 7. In the present application, the control connection is referred to as a "command channel," and the data connection is referred to a "data channel." Second, although "[t]he FTP specification says that by default, all data transfers should be over a single connection, ... most current FTP clients do not behave that way." Instead, "[a] new connection is used for each transfer; to avoid running afoul of TCP's TIMEWAIT state, the client picks a new port number each time and sends a PORT command announcing that to the server." Alternatively, "if the client sends a PASV command, the server will do a passive TCP open on some random port, and inform the client of the port number. The client can then do an active open to establish the connection." Bellovin, Firewall-Friendly FTP, Network Working Group RFC-1579, February 1994, page 1. Therefore, in practice, more than two connections are typically used for one FTP session. Third, because of the multiple-connection requirement, an FTP session through a firewall often requires the opening and closing of multiple random ports in the firewall to accommodate the data connection. That is, a firewall port randomly assigned for one FTP data connection does not remain open indefinitely. "After requested data are sent to the passive FTP client system 2 by the FTP server 4 over the data channel, the FTP server 4 and the firewall 10 dynamically close the corresponding logical communication ports until the next data channel transmission." Page 9, lines 5-9.

Further, the above-quoted passage does not say anything about restricting all data flow to a single port in the firewall. While one connection is kept open between the two proxy devices for one HTTP session, there is no suggestion that the same connection will be used for all HTTP sessions (i.e., all data flows) between the two proxy devices. As such, multiple random ports (or TCP sockets) may still be opened and closed in the firewall for multiple HTTP sessions. In the present invention, however, "a single outbound connection between the FTP client proxy system 12 and the FTP server agent 14 uses a single port on the firewall 10 and multiplexes a plurality of FTP sessions between a plurality of FTP servers 4 and a plurality of passive FTP client systems 2." Page 19, lines 2-5 (emphasis added). See also, Figures 3 and 4.

For at least these reasons, there is no basis to equate a persistent HTTP connection with a single-port FTP through a firewall. Since neither Sit nor Epstein teaches or suggests "*restricting all flow of FTP data passing through said security system through a single port on said firewall*," their combination cannot render the present invention obvious.

(2) There Is No Suggestion or Motivation to Combine or Modify Sit and Epstein

As stated in MPEP § 2143.01, obviousness can only be established by combining or modifying the teachings of the prior art to produce the claimed invention where there is some teaching, suggestion, or motivation to do so found either in the references themselves or in the knowledge generally available to one of ordinary skill in the art. In re Fine, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988); In re Jones, 958 F.2d 347, 21 USPQ2d 1941 (Fed. Cir. 1992).

Since no such "teaching, suggestion, or motivation" can be found in the cited references or in general knowledge, the obviousness rejection of the pending claims is improper.

The text of Sit does not provide any explicit suggestion or motivation to combine with Epstein. Despite the apparent similarity between the Sit system as illustrated in its Figure 5 and

the secured FTP architecture as illustrated in Figure 2 of the present application, Sit makes no reference to the terms "FTP" or "file transfer protocol." Therefore, Sit provides no explicit motivation to modify its system for FTP sessions.

Neither is there any implicit suggestion for the modification. First, Sit focuses exclusively on HTTP sessions, which, as described above, are completely different from typical FTP sessions in terms of the required number of connections and firewall ports. It is hardly obvious how such a HTTP-specific implementation could be adapted for FTP traffic. Second, Sit's primary goal is to allow an outside computer to access and control a local computer behind a firewall. To achieve this goal, Sit implements two HTTP proxies to trick the firewall into believing the incoming requests are responses to some outgoing requests. This trickery on the firewall achieves exactly what a secured FTP architecture tries to avoid. In the present invention, the security of the firewall is not in anyway circumvented or compromised. Claim 1 recites "said firewall restricting data flow between said first proxy system and said second proxy system to outbound communications through a single port on said firewall." Thus, the firewall in the present invention still functions as it is designed to. All FTP data between a local FTP client and an external FTP server are multiplexed onto a single-port secured connection between the two proxy systems. It is hard to imagine that a network engineer mindful of firewall security would be inspired by Sit's security-bypass measures to build a secured FTP system as claimed.

Nor does Epstein provide any suggestion or motivation to combine with Sit. Epstein uses an internal content-based filter to enhance security of a multi-part proxy based firewall or guard. A single FTP proxy is included in the multi-part proxy. See Epstein: Figures 2 and 4. Such traditional single-proxy FTP application is not amenable to adaptation in the two-HTTP-proxy environment as disclosed in Sit.

The Examiner cites the following passage to suggest that Epstein is readily combinable with Sit:

> "Proxy server 200 generally includes an operating system 204 (possibly hardened) operating on computing hardware 202. Proxy server 200 also includes a plurality of proxy applications, shown in FIG. 2, including, for example, HTTP proxy application 206A, SMTP proxy application 206B, and FTP proxy application 206C." Epstein: col. 4, lines 16-20.

However, apart from briefly mentioning "HTTP proxy application" and "FTP proxy application" in the same sentence, this passage has no relevance to the Sit patent. In fact, in this passage and in six other instances where the term "FTP" is used (i.e., Epstein: col. 1, line 37; col. 2, line 27; col. 4, lines 4-5 and 10), Epstein only refers to well-known standard FTP operations and regular FTP proxies. Other than listing FTP proxy application as one possible component in a multi-part proxy, Epstein says nothing that is even remotely related to Sit's two-HTTP-proxy setup or the present invention's two-FTP-proxy architecture.

Since neither Sit nor Epstein provides any motivation to combine, in order for the obviousness rejection to stand, such motivation must come from the knowledge generally available to one of ordinary skill in the art. However, that is not the case either. In order to solve the problems uniquely associated with FTP sessions through a firewall, an artisan must first identify such problems. As recognized in the present application, the specific problems include, for example, the "potential security exposures" caused by "dynamic opening and closing of ports on a firewall," and the "significant administrative resources" "required to configure a firewall to allow communication over a large range of sources and destinations." Page 9, lines 17-21. The recognition of such problems is an essential part of the present invention, which leads to a secured FTP architecture as recited in claims 1 and 12. Yet, there is no indication in the cited

references that these problems were ever recognized or identified prior to the time of the present invention. Nor are these problems easily recognizable by a person of ordinary skill in the art.

Further, the HTTP-based Sit system cannot be mechanically combined with Epstein for implementation of a secured FTP system as claimed. Even if Sit and Epstein were combinable, the mere fact that references can be combined or modified does not render the resultant combination obvious unless the prior art also suggests the desirability of the combination. In re Mills, 916 F.2d 680, 16 USPQ2d 1430 (Fed. Cir. 1990). Without a clear recognition of the problems associated with FTP sessions through a firewall, the desirability of the combination is not apparent from the cited references.

Since the requisite suggestion or motivation is not found in the references themselves or in the knowledge generally available to one of ordinary skill in the art, the Office Action has failed to establish a prima facie case of obviousness. Withdrawn of the obviousness rejection is respectfully solicited.

C. CONCLUSION

For at least the reasons provided above, Applicant respectfully submits that the application is in condition for allowance. Favorable reconsideration and allowance of the pending claims are respectfully solicited.

Should there be anything further required to place the application in better condition for allowance, the Examiner is invited to contact Applicant's undersigned representative at the telephone number listed below before issuance of any further office action.

In the event any additional fees are due, the Commissioner is hereby authorized to charge the undersigned's Deposit Account No. 50-0206.

Respectfully submitted,

HUNTON & WILLIAMS, LLP

By: _____
Co-Li
Registration No. L0214

Hunton & Williams, LLP
1900 K Street, N.W., Suite 1200
Washington, D.C. 20006-1109
Telephone (202) 955-1500
Facsimile (202) 778-2201

Dated: 8/29/05